Remarks

Reconsideration of the above referenced application in view of the enclosed amendment and remarks is requested. Claims 1, 6, 9, 17, 19, and 29 have been amended. Claims 31-38 stand withdrawn. Claims 1-30 and 39-40 are pending in the application.

ARGUMENT

Claim 9 is rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement. This rejection is respectfully traversed as discussed below and Claim 9 and its progeny are believed allowable, as amended.

The Examiner asserts that the claimed subject matter was not described in the Specification as originally filed. This assertion is in error. Specifically, the Examiner asserts that the PCX module being configured to process disparate data stream protocols is new matter. Applicants respectfully direct the Examiner to, at least, pages 8-11. On page 8 of the specification, it is described that:

> "PCX module 106 includes a number of protocol specific exchange modules 130. Protocol specific encrypted data is received over protocol specific bus 120 from protocol specific input devices 110. In the Figure 1 example, encrypted data may be received over a 1394 DTCP bus from a number of input devices 110 such as a satellite dish or video recorder (VCR). Any of a number of protocol specific buses 120 may be connected to data safeguarding device 104 including, for example, a USB bus, a PCI bus, and a DVD bus. Once the encrypted data is received by data safeguarding device 104, CPU 115 directs the input to PCX module 106. Within PCX module 106, the appropriate protocol specific exchange module 130 is used to decrypt the encrypted input data stream. For example, if IEEE 1394 DTCP bus encrypted data is received, a DTCP exchange module 130 would be used to decrypt the input data. Input data is received and is decrypted on a block-by-block basis." [emphasis added]

On page 10, the specification describes that the disparate data stream data is re-encrypted and then forwarded to the appropriate decoder device, for instance an MPEG device or AC3 device.

> "The re-encrypted data is transferred to a splitter 232 which splits the data between the various decoding devices. In the figure 2 example, the splitter 232 splits the

IEEE 1394 re-encrypted data to AC3 device 216 and MPEG device 218. MPEG decoder 218 and AC3 decoder 216 receive the appropriate encrypted PCX content key. MPEG decoder 218 and AC3 decoder 216 decrypt their PCX content key with their PCX session key. MPEG device 218 and AC3 device 216 then decrypt the re-encrypted data for playback using the appropriate PCX content key."

On pages 11-12 it is described that:

"...Within PCX module 106, the encrypted protocol specific data is decrypted using protocol specific decryptor 322. Protocol specific decryptor 322 decrypts the protocol specific data one block at a time. Each block of data contains a transmission header portion and a payload. In one embodiment, both the transmission header and payload portions are encrypted during transmission from source device 110 to data safeguarding system 100. In an alternate embodiment, only the payload may be encrypted. Depending on the specific data bus transmission protocol being used, protocol specific decryptor 322 decrypts either the entire data block or the payload only.

Each data bus transmission protocol requires a corresponding protocol specific decryptor 322. PCX negotiator 328 negotiates a PCX session key with the decoding device 102 that is the intended recipient of the protocol specific data. Once a session key is negotiated, protected content exchange (PCX) encryptor 324 re-encrypts the payload portion of the data with a randomly generated PCX content key to produce re-encrypted data. PCX encryptor 324 transfers the re-encrypted data to protocol specific bus abstractor 320 which, in turn, transfers the re-encrypted data to device specific mini port driver 316. Device specific mini port driver 316 sends the PCX re-encrypted data to the upstream drivers and libraries 330 which in turn transfers the PCX re-encrypted data to splitter 232."

As will be appreciated by one of ordinary skill in the art, the PCX module is configured to receive data streams from a variety of disparate devices, each potentially having a disparate protocol. The PCX may include protocol specific exchange modules to appropriately decode the data stream from disparate sources, or data streams. For instance, data streams from a USB, PCI or DVD bus are specifically described. It will also be understood by one of ordinary skill in the art that a disparate number of devices may send a data stream to the PCX module. As described in the specification, the data may include both MPEG and AC3 data, having disparate protocols. This disparate data is decoded and split to be forwarded to the appropriate device based on the header information in the disparate protocols. As will be understood by one of skill in the art, these protocols are meant to be illustrative and Applicants' claimed invention is not limited to these enumerated protocols.

The subject matter alleged to be missing from the specification was indeed present in the description as originally filed. However, the Examiner fails to provide a prior art reference that teaches or suggests this limitation. Therefore, Applicants respectfully request that the Examiner remove the finality of the present office action and provide a new office action addressing this limitation. Further, this limitation has been added to the other independent claims. Since the subject matter was present in the Specification as filed, the Examiner was obligated to search for this feature in response to the previous Amendment. Therefore, an Advisory Action asserting a new search is required would be improper. Applicants respectfully request that a new office action be issued addressing all of the added limitations and features of the previous Amendment, even if they were added to independent claims in the present Amendment.

Claims 9-16 are rejected under 35 U.S.C. 112, second paragraph as being incomplete for omitting essential steps. This rejection is respectfully traversed and claims 9-16 are believed allowable prior to amendment. However, in order to expedite allowance of the present application, Applicants amend claim 9 to include the alleged missing element. Claims 9-16 are believed allowable as amended.

Claims 9-16 are rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,757,908 to Cooper et al., (hereafter, "Cooper et al."). This rejection is respectfully traversed and Claims 9-16 are believed allowable based on the above amendments and the foregoing and following discussion.

Generally, Cooper et al. teach a system for enabling a file or software application which has been locked from the user. Cooper et al. teach an apparatus for securing access to particular files which are stored in a computer-accessible memory media. A plurality of files is stored in a computer-accessible memory media, including at least one file previously encrypted by the vendor, and at least one unencrypted file. For each encrypted file, a *preselected portion of the file* is recorded in memory, a decryption block is generated which includes information which can be utilized to decrypt the file, and the decryption block is incorporated in the file in lieu of the *preselected portion* which has been recorded in memory. This entire file is then distributed to the user. Cooper et al. does not teach a system which receives an encrypted data block, decrypts the data block, replaces a portion of a decrypted data block, and then re-encrypts one or more

portions of the decrypted data block with an encryption key to retransmit within the system to maintain security of the data block while moving through the system.

In contrast, Applicants' invention recites a system for transmitting a data stream made up of data blocks, where a data block portion of a payload may be replaced with a tag indicating whether a decryption key is necessary to decode the data block. The data blocks of a given data stream may contain disparate protocols and be routed to one or more application decoders. Further, the sending device and receiving device may negotiate for a session key to decrypt the decryption keys, thereby enabling additional security to the data stream as is passes through the data safeguarding device. This negotiation is specifically claimed in the provisionally withdrawn claims.

Cooper et al. teach a system where only one portion of a file is encrypted to protect it from being accessed by a user upon a user request to access the file. An operating system level file management program determines whether the user is authorized to access the file and supplies the decryption key. Cooper et al. teach supplying the key by the vendor. Cooper et al. do not teach or suggest a *decrypted data stream* received from a source device, but merely a file drawn from media.

As described in the specification, and recited in the claims, Applicants' invention safeguards data within a device and forwards data of varying protocols to appropriate application decoders. If a data stream contains both audio and video data blocks, the data blocks from the received data stream may be sent to different application decoders based on their protocol, i.e., audio vs. video formats. Applying the teachings of Cooper et al. to Applicants' invention will result in an operating system level decoder for files and not a safeguarding device that may be implemented in hardware, software, or firmware that receives transmitted data streams without user request.

The Examiner asserts that Cooper et al. disclose all elements of the claims. The independent claims have been amended to more clearly recite that the sending system, receives an encrypted data block from a protocol specific input device, decrypts the data block and then re-encrypts at least portions of the data block before sending the encrypted data to the second system, i.e., the application decoder module. This encrypting of the data is a second encrypting, or *re-encrypting*. The data block is not received in an encrypted mode and then merely passed

through to the second system. It is first decrypted. After decrypting by the first device, a portion of the payload may be replaced. At least a portion of the data block is encrypted before transmitting to the second device. Cooper et al. do not teach or suggest this decrypting and re-encrypting. Further, because the payload may be encrypted independently of the header information, the decrypting and re-encrypting may significantly alter the data stream.

Cooper et al. do not teach a method to re-encrypt a decrypted data stream, but only a method to decrypt a pre-encrypted file on a media device. In contrast, Applicants' claimed invention decrypts an encrypted data stream and re-encrypts the payload portion of the data blocks in the data stream before sending them to one or more application decoders. The PCX and application decoders may be separate devices, circuits or modules, or they may be part of the same device. Regardless, the PCX and application decoders are part of an overall data safeguarding system. Cooper et al. teach that the encryption occurs on a vendor system and decryption occurs on a user system. Further, since the Examiner fails to address the limitation of *wherein the sending system comprises a protected content exchange (PCX) module configured to process disparate data stream protocols routed to one or more application decoder modules based on a protocol corresponding to the data block, and wherein the receiving system comprises at least one application decoder module,* this rejection is improper and fails to show a prima facie case of anticipation. Thus, Claims 9-16 are allowable as amended.

Claims 1-8, 17-30 and 39-40 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 5,572,442 to Schulhof et al. (hereinafter "Schulhof et al.") in view of Cooper. This rejection is respectfully traversed and Claims 1-8, 17-30 and 39-40 are believed allowable based on the above amendments and the following discussion.

Schulhof et al. teach a distribution system for audio materials including a portable audio storage. Schulhof et al. teach that an encrypted data stream may be received from an input program signal. The data stream is decrypted, demodulated and decoded as necessary so that it can be stored on the portable storage device. However, once decrypted and stored, the data is susceptible to unauthorized access and manipulation. There is no guarantee that the stored data will maintain its integrity. In contrast, Applicants' invention passes the encrypted data blocks through a safeguarded system without storing them unprotected on a media device.

The Examiner's cited reference (Col. 11, lines 42-55) merely teach that the system receives an encrypted or encoded data stream which is decrypted or decoded before storing on a portable storage medium. The portable medium taught by Schulhof et al. contains unencrypted data, and is meant to be transportable to be used by multiple systems. This teaches away from Applicants' claimed system which safeguards the data by re-encrypting at least a portion of the payload before transmitting it to another device. The Examiner's Official Notice that encryption is frequently used is not relevant to the Applicants' claimed invention. A combination of Cooper et al., Schulhof et al., and encryption generally, will not result in Applicants' claimed invention. None of the cited references (even with the Official Notice) either alone or in combination teach a system that may receive disparate encrypted data streams, protect the data content while forwarding through a system with re-encryption and negotiation of keys, and then forward the received data blocks to a protocol specific application decoder.

Combining the teaching of Schulhof et al. and Cooper et al. will not result in Applicants' claimed invention. If Cooper et al. were to retrieve data from the Schulhof et al. portable storage, it is the equivalent of retrieving an open data stream and not a decrypted data stream which has been re-encrypted, at least in part. Schulhof et al. do not suggest that the portable storage device stores anything other than the original unencrypted data stream. Schulhof et al. merely suggest that the data might be received in an encrypted format and that decrypting, decompressing and decoding take place as necessary. This teaching implies that the data stored on the portable media device is placed in its original state, and accessible to any process having access to the device and thus susceptible to being read by, or modified by, any unauthorized system or device.

In contrast, Applicants' invention safeguards the data in the data stream within a device having a sending system and receiving system. Encrypted or partially encrypted data is received from a protocol specific device and then decrypted and re-encrypted with a flag to so indicate. It is then sent to through the device to the receiving system in an encrypted state. At no time is the data stream susceptible to being read in an unencrypted state by another process. The system as taught by Schulhof et al., allows the data stream to be read or modified by another process. Therefore, combining the teachings of Schulhof et al. and Cooper et al. cannot result in Applicants' claimed invention.

Further, combining the two references is improper as Cooper et al. teach installing trial software and Schulhof et al. teach distributing audio and video programming. There is no motivation to combine these teachings. Cooper et al. do not teach or suggest that their process may use audio and video programming, but only software code. Schulhof et al. teach only audio data. Neither reference teaches receiving and forwarding data having disparate protocols. Cooper et al. also teach using pre-selected encrypted portions of software. Cooper et al. teach that the software is received as reversibly functionally limited software. The pre-selected portions are received by the user in an encrypted state. Combining the teachings of Schulhof et al. would result in Cooper et al. receiving unencrypted and wide open software code which would negate the purpose of having functionally limited software distributed to users. Thus, the combination of the references is improper and Claims 1-8, 17-30 and 39-40 are believed allowable.

Thus, for the foregoing reasons, all claims remaining in the application are now allowable.

CONCLUSION

In view of the foregoing, Claims 1-30 and 39-40 are all in condition for allowance. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (703) 633-6845. Early issuance of Notice of Allowance is respectfully requested. Please charge any shortage of fees in connection with the filing of this paper, including extension of time fees, to Deposit Account 02-2666 and please credit any excess fees to such account.

Respectfully submitted,

Dated: 13 April 2006

/ Joni D. Stutman-Horn /

Joni D. Stutman-Horn, Reg. No. 42,173
Patent Attorney
Intel Corporation
(703) 633-6845

c/o Blakely, Sokoloff, Taylor & Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1030